Amendment to the Claims

Applicant respectfully requests the following amendments to the claim set:

1. (Previously Amended) A control device for authenticating the identification of a user prior to access to a software application, the control device comprising:

a) a biometric signal acquisition module located on a computer input device;

b) an area on the computer input device through which the biometric acquisition module may obtain the biometric signal of a user in control of the computer input device; and

c) an independent software interface capable of being imposed on an operating system or on an individual software application for comparing the acquired biometric signal to a collection of authorized signals to determine if the individual controlling the computer input device is authorized to access the operating system or the software application, wherein the software interface controls access to the operating system or software application based on a comparison of the acquired biometric signal to the collection of authorized signals.

2. (Previously Amended) A method for preventing access to a software application the method comprising the steps of: (a) providing an independent software interface capable of being imposed on an operating system or on an individual software application; (b) obtaining a baseline biometric signal from an authorized user into the software interface; (c) obtaining through a biometric acquisition module located in a computer input device a current biometric signal from an individual controlling the computer input device; (d) comparing the current biometric signal with the baseline biometric signal to determine whether the individual is authorized to access the operating system or software application; and (e) controlling access to

the operating system or software application with the software interface based on a comparison of the baseline biometric signal and the current biometric signal.

3. (Previously Amended) A method for providing security to a network of computers, the method comprising of steps of (a) providing an independent software interface capable of being imposed on an operating system or on an individual software application; (b) obtaining baseline biometric signals for all authorized users of a network; (c) providing a biometric acquisition device in a computer input device operated by the hand of a user at the location of each of the authorized users; (d) obtaining a current biometric signal through the computer input device from an individual attempting to access the network; (e) comparing the current biometric signal with the stored baseline biometric signals to determine whether the individual is authorized to access the network; and (e) controlling access to the network with the software interface based on a comparison of the baseline biometric signals and the current biometric signal.

4. (Cancelled)

5. (Previously amended) The method set forth in the claim 3 above further comprising the steps of (f) storing the current biometric signal from an unauthorized user attempting to access the network beyond the time necessary for the steps of comparing the current biometric signal with the stored baseline biometric signals and controlling access to the

network with the software interface and (g) providing the stored current biometric signal to the manager of the network.

6-8. (Cancelled)

9. (Previously Presented) A control device as in claim 1 above, wherein the software interface sends a message to the user of the software interface notifying the user of inappropriate access attempts.

10. (Previously Presented) A control device as in claim 1 above, wherein the software interface stores the acquired biometric signal for a period of time longer than that necessary to compare the acquired biometric signal to the collection of authorized signals to permit identification of the individual who inappropriately attempted to access the operating system or the software application.

11. (Previously Presented) A method of preventing access to a software application as in claim 2 above further comprising the step of sending a message to the authorized user notifying the authorized user of inappropriate access attempts.

12. (Previously Presented) A method of preventing access to a software application as in claim 2 above further comprising the step of storing the current biometric signal for a period of time longer than that necessary to compare the current biometric signal with the baseline biometric signal and the period of time necessary to control access to the operating

system or software application to permit identification of the individual attempting to use the operating system or software application.

13. (Previously Presented) A method of preventing access to a software application as in claim 12 above further comprising the step of using the stored current biometric signal to identify the individual attempting to use the operating system or software application.

14. (Previously Presented) A method of preventing access to a software application as in claim 13 above further comprising the step of using an identification of the individual attempting to use the operating system or software application to determine the access habits of the individual attempting to use the operating system or software application.